Defence Research and Development Canada
Recherche et développement pour la défense Canada

DEFENCE R&D DÉFENSE

Assessing Vulnerability of Biometric Technologies for Identity Management Applications

Final Report

Prepared by:
Drew Smeaton
Communications Security Establishment Canada

Raj Nanavati
International Biometric Group

Scientific Authority:
Pierre Meunier
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science
Contractor Report
DRDC CSS CR 2011-19
October 2011

Canada

Assessing Vulnerability of Biometric Technologies for Identity Management Applications

Final Report

Prepared by:
Drew Smeaton
Communications Security Establishment Canada

Raj Nanavati
International Biometric Group

Scientific Authority:
Pierre Meunier
DRDC Centre for Security Science

Defence R&D Canada – Centre for Security Science

Contractor Report
DRDC CSS CR 2011-19
October 2011

Principal Author

Original signed by Drew Smeaton

Drew Smeaton

Manager Research and Prototyping L2C

Approved by

Original signed by Jack Pagotto

Jack Pagotto

DRDC CSS Section Head

Approved for release by

Original signed by Dr. Mark Williamson

Dr. Mark Williamson

DRDC CSS DDG -DRP Chair

In conducting the research described in this report, the investigators adhered to the policies and procedures set out in the Tri-Council Policy Statement: Ethical conduct for research involving humans, National Council on Ethics in Human Research, Ottawa, 1998 as issued jointly by the Canadian Institutes of Health Research, the Natural Sciences and Engineering Research Council of Canada and the Social Sciences and Humanities Research Council of Canada.

Abstract

To address the Community of Practice (CoP) objective of evaluating the utility of potential biometrics techniques that could be used to enhance the security of Information Technology (IT) systems, including Supervisory Control And Data Acquisition (SCADA) systems and e-Government services, the Study Team for PSTP-02-336BIOM developed a framework for addressing biometric vulnerabilities, researched case study examples of existing deployed biometric systems, and conducted a small-scale evaluation to compare the utility of biometrics vs. passwords.

In developing the framework, the Study Team researched existing biometric evaluation frameworks to identify gaps, and synthesized a practical framework aimed at an audience of IT security practitioners, with the intent of addressing the growing use of biometrics in government applications and the implications that it has on IT systems security.

The Study Team also conducted a preliminary comparative evaluation of the utility of biometrics vs. passwords as a single-factor authentication method using experimental test trials and a user survey. Comparison criteria included: whether or not user access is granted, number of attempts, and usability. The evaluation confirmed experimentally that single-factor biometric technology is a viable and user-accepted means of authentication for IT system access that is at least as fast and reliable as username-password methods.

Résumé

Pour atteindre l'objectif de la communauté des praticiens (CP) d'évaluer l'utilité des techniques de biométrie qui pourraient être utilisées pour améliorer la sécurité des systèmes informatiques, y compris les systèmes SCADA (télésurveillance et acquisition de données), et les services e-gouvernement, l'équipe d'étude pour PTSP-02-336BIOM a élaboré un cadre pour s'attaquer aux vulnérabilités biométriques, a fait des recherches sur des études de cas des systèmes biométriques existants déployés, et a mené une évaluation à petite échelle pour comparer l'utilité de la biométrie contre les mots de passe.

Dans l'élaboration du cadre, l'équipe d'étude a fait des recherches sur des cadres d'évaluation biométrique existants pour identifier les lacunes, et a synthétisé d'un cadre pratique destiné aux professionnels de la sécurité de technologies de l'information (TI), avec l'intention de s'attaquer à l'utilisation croissante de la biométrie dans les applications gouvernementales et les conséquences qu'elle a sur les systèmes de sécurité de TI.

L'équipe d'étude a également effectué une évaluation comparative préliminaire de l'utilité de la biométrie contre les mots de passe en tant que méthode d'authentification à un seul facteur à l'aide d'essais expérimentaux et une enquête auprès des utilisateurs. Les critères de comparaison ont compris : si ou non l'accès des utilisateurs est accordé, le nombre d'essais, et la facilité

d’utilisation. L’évaluation a confirmé expérimentalement que la technologie biométrique seul-doigt est un moyen viable et acceptée par l’utilisateur d’authentification pour l’accès au système informatique qui est au moins aussi rapide et fiable que les méthodes de nom d’utilisateur-mot de passe.

Executive summary

Assessing Vulnerability of Biometric Technologies for Identity Management Applications: Final Report

Smeaton, D.; Nanavati, R.; Wong, B.; Waung, D.; Coleman, D., Hart, C.; Unwala, A.; DRDC CSS CR CR-2011-19; Defence R&D Canada – CSS; October 2011.

Background and Objectives: The Defence Research and Development Canada (DRDC) Public Security Technical Program (PSTP) maintains a Surveillance, Intelligence, and Interdiction (SI^2) Domain. Within this Domain, two investment priorities were identified under the Biometrics for National Security Community of Practice (CoP) as part of PSTP Call for Proposals 2 in December 2009. The first Statement of Work (SOW), "Role of Biometrics in Identity Management for IT System Access Control", describes an assessment of biometric options in identity assurance framework as it relates to IT systems, including SCADA systems and e-government services, and vulnerability testing & analysis of the relationship between system performance and security strength of function. In October 2010, IBG-Canada was awarded contract PSTP-02-336BIOM to execute a Study on this topic. Communications Security Establishment Canada (CSEC) served as the Lead Federal Department for the Study, and IBG-Canada served as the Lead Applicant. Other Study Partners included: Canada Border Services Agency (CBSA), Foreign Affairs and International Trade Canada (DFAIT), DRDC-Toronto, Office of the Privacy Commissioner of Canada (OPC), Royal Canadian Mounted Police (RCMP), Transport Canada, University of Toronto (U of T) / Identity, Privacy and Security Institute (IPSI), GenKey, priv-ID, and Reboot Communications.

Agencies and departments within the Government of Canada need information on the performance, vulnerabilities and effectiveness of biometric solutions for identity management access control applications, including SCADA systems and e-Government services. Documents such as Information Technology Security Guidance ITSG-31 *User Authentication Guidance for IT Systems* notwithstanding, few guidance documents consider biometrics as a robust standalone authentication technique. Product-focused evaluation frameworks are costly and time-consuming, and overlook human elements that can drive performance, security, and vulnerabilities. An improved framework that incorporates biometric–based factors improves the CoP's ability to operationalize biometric technologies.

Therefore, the first objective of the Study was to evaluate the potential vulnerability and utility of biometric technologies for Government use in IT system access control applications and e-Government services. This objective addressed the Biometric CoP's goal to evaluate, analyze, and support biometric technology implementations that enhance national capabilities.

The second objective was to improve the ability of Canadian Government Agencies to identify and mitigate security vulnerabilities and privacy risks, and preserve interoperability in ID management systems, by producing guidance for decision-makers with respect to deploying biometric technology as a method for single-factor authentication.

Framework Development: Building upon CSEC's *Technical Research Report on Biometrics for Authentication for Enterprise Security Architectures*, and input from CSEC, OPC and other

Federal partners, IBG's team of technology experts, researchers and analysts compared the utility of biometrics against other authentication methods such as passwords and cryptographic tokens.

The project team conducted a survey of existing biometric vulnerability assessment frameworks, as well as recent privacy policy documents, reviewing common IT evaluation frameworks and identifying gaps. These frameworks included: the Common Criteria for Biometric Evaluation Methodology Supplement (BEM), ISO/IEC 19792 *Security evaluation of a biometric system*, and CSEC ITSG-31 *User Authentication Guidance for IT Systems*.

The project team then synthesized a practical framework aimed at IT security practitioners, who may not be familiar with biometrics as an authentication method. The framework will help practitioners and decision-makers understand and evaluate biometric technologies as a viable method for authentication.

Case Study Analyses: Case study analyses were conducted by researching deployed operational biometric systems in Canadian and international settings and describing them in terms of metrics discussed in the synthesized and existing frameworks. These descriptions serve as examples of successful deployments of biometrics for applications that may be of interest to the Government of Canada.

Comparative Evaluation: For the comparative evaluation, the Study team developed a test methodology and plan for directly comparing the utility of biometric authentication to password authentication through an experimental test using a small set of Test Subjects and trials. The project team built a test platform that simulates the user login experience using a representative fingerprint biometric system and a username-password authentication system, while collecting measurable criteria such as:

- Whether access was granted;
- Number of attempts before gaining access; and
- Time to authenticate.

Data on additional metrics such as ease-of-use and user acceptance were collected using a user survey conducted after the test trials. At the end of the evaluation, the recorded data was aggregated and analyzed.

Evaluation Results: The test results confirmed experimentally that single-factor biometric technology is a viable and user-accepted means of authentication for IT system access that is at least as fast and accurate as username-password methods. The test results also suggested that the performance of the biometric technology may be better than that of username-password methods in terms of a higher proportion of successful access attempts for daily as well as intermittent use.

The test results and user survey showed that a large number of Test Subjects wrote down their passwords, used "weak" passwords that were easier to remember, and/or used the same password for multiple systems, potentially compromising the strength of the username-password authentication.

These results support the evaluation and confirmation of the utility of a representative biometric technology for IT access control and access to e-Government services, supporting the primary

SOW objective. However, further study on a larger scale with a larger and more diverse subject population is recommended to strengthen the conclusions.

Significance and Future Plans: The Study concludes that, when deploying authentication systems for IT network access, it is important that organizations examine biometrics as a valid method of authentication, in addition to more traditional methods. IT security professionals may have the "pre-programmed" mindset to utilize usernames and passwords as a method of authentication, because of widespread use, ease of implementation, and comparatively low costs of implementation. Unfortunately, username-password may not be the most secure form of authentication due to mature tools used by attackers to exploit password vulnerabilities such as Trojan horses and key-loggers.

The deliverables of the Study facilitate the assessment of potential biometric authentication solutions across the Personnel Research and Development and Operations Research; Infrastructure and Organization; Concept, Doctrine and Collective Training; Information Management; and Equipment, Supplies and Services (PRICIE) spectrum, by identifying gaps in existing security evaluation methodologies and synthesizing a best-of-breed evaluation framework that incorporates privacy issues. Study results will inform IT security and privacy policy development, and facilitate deployment of biometric technologies as standalone authentication methods and in conjunction with other mechanisms for multi-factor authentication systems.

This impact is expected to include the security and privacy of practitioner and beneficiary access to electronic health information through systems such as Canadian Forces Health Information System (CFHIS), using biometrics alone or in conjunction with authentication mechanisms such as electronic versions of the Canadian Forces ID, Canadian Forces Health Care ID, or Canadian Forces Military Family ID.

In addition to the direct results of the evaluation, the test methodology and plan developed in the Study, as well as the test application design, can be used to conduct the, more in-depth comparison.

Sommaire

Assessing Vulnerability of Biometric Technologies for Identity Management Applications: Final Report

Smeaton, D.; Nanavati, R.; Wong, B.; Waung, D.; Coleman, D., Hart, C.; Unwala, A.; DRDC CSS CR CR-2011-19; R & D pour la défense Canada – CSS; Octobre 2011.

Contexte et objectives: Le Programme technique de sécurité publique (PTSP) de Recherche et développement pour la défense Canada (RDDC) maintient un domaine de Surveillance, renseignement et interdiction (SRI). Dans ce domaine, deux priorités d'investissement ont été identifiés dans la communauté des praticiens (CP) en biométrie au profit de la sécurité nationale dans le cadre du PTSP Appel à propositions 2 en Décembre 2009, avec le premier énoncé, «Le rôle de la biométrie dans la gestion des identités pour contrôle d'accès aux systèmes informatiques », décrivant l'évaluation des options biométriques dans le cadre d'assurance de l'identité en ce qui concerne les systèmes informatiques, y compris les systèmes SCADA et des services e-gouvernement, et des tests de vulnérabilité et d'analyse de la relation entre la performance du système et la force de sécurité de la fonction. En Octobre 2010, IBG-Canada a obtenu un contrat, PTSP-02-336BIOM, pour exécuter une étude sur ce sujet. Le Centre de la sécurité des télécommunications Canada (CSTC) a servi de principal ministère fédéral pour l'étude, et IBG-Canada a été le candidat principal. Autres Partenaires de l'étude comprenaient: l'Agence des services frontaliers du Canada (ASFC), Affaires étrangères et Commerce international Canada (MAECI), RDDC-Toronto, le Commissariat à la protection de la vie privée du Canada (OPC), la Gendarmerie royale du Canada (GRC), Transports Canada, U de T / IPSI, GenKey, priv-ID, et Reboot Communications.

Les agences et ministères du gouvernement du Canada ont besoin d'information sur la performance, les vulnérabilités et l'efficacité des solutions biométriques pour les applications de gestion des identités pour contrôle d'accès, y compris les systèmes SCADA et des services e-gouvernement. Les documents tels que ITSG-31 *Guide sur l'authentification des utilisateurs pour les systèmes TI*, nonobstant, peu de documents d'orientation considèrent la biométrie comme une technique d'authentification robuste autonome. Les cadres d'évaluation axée sur les produits sont coûteux et fastidieux, et négligent des éléments humains qui peuvent stimuler la performance, de sécurité et les vulnérabilités. L'amélioration du cadre qui intègre des facteurs biométriques à base améliore la capacité de la Communauté de praticiens en vue de concrétiser les technologies biométriques.

Par conséquent, le premier objectif de l'étude était d'évaluer la vulnérabilité potentielle et l'utilité des technologies biométriques pour l'utilisation dans les applications informatiques du gouvernement du système de contrôle d'accès et de services e-gouvernement. Cet objectif adressée l'objectif de la CP en biométrie pour évaluer, analyser, et soutenir les implémentations de la technologie biométrique qui renforcent les capacités nationales.

Le deuxième objectif était d'améliorer la capacité des organismes gouvernementaux canadiens pour identifier et atténuer les failles de sécurité et les risques de confidentialité, et de préserver l'interopérabilité des systèmes de gestion d'identité, en produisant des conseils pour les décideurs

en ce qui concerne le déploiement de la technologie biométrique comme méthode d'authentification avec un seul facteur.

Cadre de développement: Tirant parti du rapport de recherche technique du CSTC sur la biométrie pour l'authentification pour les architectures d'entreprise de sécurité (*Technical Research Report on Biometrics for Authentication for Enterprise Security Architectures*), et la contribution de l'CSTC, OPC et d'autres partenaires fédéraux, les experts en technologie, les chercheurs et les analystes de l'équipe d'étude d'IBG ont fait des recherches sur l'utilité de la biométrie contre autres méthodes d'authentification telles que mots de passe et jetons cryptographiques.

L'équipe d'étude a mené une enquête auprès des cadres existants pour évaluation des vulnérabilités biométriques, ainsi que des documents récents politique de confidentialité, l'examen des cadres d'évaluation communs d'informatique et identifier les lacunes. Ces cadres inclus: Critères communs pour l'évaluation du supplément biométrique Méthodologie (BEM), ISO / IEC 19792 *Cadre de la sécurité pour l'évaluation et le test de la technologie biométrique*, et CSTC ITSG-31 *Guide sur l'authentification des utilisateurs pour les systèmes TI*.

L'équipe d'étude a ensuite synthétisé un cadre pratique visant aux praticiens de la sécurité informatique, qui peut ne pas être familiers avec la biométrie comme méthode d'authentification. Le cadre aidera les praticiens et les décideurs à comprendre et évaluer les technologies biométriques comme une méthode viable pour l'authentification.

Analyses d'études de cas: Des études de cas ont été menées par des recherches sur des systèmes biométriques opérationnelles déployées dans les milieux canadiens et internationaux, et par les décriant en termes de paramètres d'évaluation examinés dans les cadres existants et synthétisés. Ces descriptions sont des exemples de déploiements réussis de la biométrie pour des applications qui peuvent être d'intérêt pour le gouvernement du Canada.

Évaluation comparative: Pour l'évaluation comparative, l'équipe d'étude a développé une méthodologie et un plan d'essai pour comparer directement l'utilité de l'authentification biométrique contre l'authentification mot de passe avec une expérimentation utilisant un petit ensemble de sujets de test et d'essais. L'équipe d'étude a créé un logiciel de test qui simule l'expérience d'utilisateur de connexion en utilisant un système représentatif d'empreintes digitales biométriques et un système d'authentification nom d'utilisateur-mot de passe, tout en collectant des critères mesurables telles que:

- Si l'accès a été accordé;
- Nombre de essais avant accédant accès; et
- Temps pour authentifier.

Données sur mesures supplémentaires telles que la facilité d'utilisation et l'acceptation par les utilisateurs ont été ramassées par un sondage mené après les essais. À la fin de l'évaluation, les données enregistrées ont été regroupées et analysées.

Résultats de l'évaluation: Résultats de l'évaluation: Les résultats des tests ont confirmé de façon empirique que la technologie à un seul facteur biométrique est un moyen viable et acceptée par l'utilisateur d'authentification pour l'accès au système informatique qui est au moins aussi rapide

et précis que les méthodes de nom d'utilisateur-mot de passe. Les résultats des tests ont également suggéré que la performance de la technologie biométrique peut être meilleure que celle des méthodes de nom d'utilisateur / mot de passe en termes d'une proportion plus élevée de essais d'accès avec succès pour tous les jours ainsi que l'utilisation intermittente.

Les résultats des essais et le sondage des utilisateurs ont montré qu'un grand nombre de sujets de test mis par écrit leurs mots de passe, ont utilisé des mots de passe «faibles» qui ont été plus faciles à mémoriser, et / ou ont utilisé le même mot de passe pour plusieurs systèmes, ce qui pourrait compromettre la résistance du nom d'utilisateur / mot de passe d'authentification.

Ces résultats soutiennent l'évaluation et la confirmation de l'utilité d'une technologie représentant biométrique pour contrôle d'accès informatique et de l'accès aux services e-gouvernement, en soutenant l'objectif principal de l'énoncé des travaux. Cependant, une étude plus approfondie sur une plus grande échelle avec une population de sujets plus nombreux et diversifié est recommandé pour renforcer les conclusions.

Importance et plans pour l'avenir: L'étude conclut que, lors du déploiement de systèmes d'authentification pour l'accès au réseau informatique, il est important que les organisations examinent la biométrie comme une méthode valable de l'authentification, en plus des méthodes plus traditionnelles. Les professionnels de la sécurité informatique peut avoir l'état d'esprit « préprogrammé » d'utiliser les noms d'utilisateur et mots de passe en tant que méthode d'authentification, à cause de l'utilisation étendue, la facilité d'implémentation, et les coûts d'implémentation relativement faibles. Malheureusement, nom d'utilisateur / mot de passe ne peut être la forme la plus sûre d'authentification en raison d'outils utilisés par des attaquants afin d'exploiter les vulnérabilités de passe tels que les chevaux de Troie et les enregistreurs de touches.

Les livrables de l'étude faciliter l'évaluation du potentiel des solutions d'authentification biométrique dans tout le spectre « PRICIE », en identifiant les écarts dans les méthodes d'évaluation de sécurité et de la synthèse d'un cadre d'évaluation meilleur-du-genre qui intègre les questions de la vie privée. Les résultats de l'étude informeront le développement de la politique sur la sécurité informatique et la vie privée, et faciliteront le déploiement des technologies biométriques comme méthodes d'authentification autonome et en collaboration avec d'autres mécanismes pour les systèmes d'authentification multi-facteur.

Cet impact devrait inclure la sécurité et la vie privée de l'accès des praticiens et des bénéficiaire à l'information de santé électronique au moyen de systèmes tels que le Système d'information de santé des Forces Canadiennes (SISFC), en utilisant la biométrie seul ou en conjonction avec des mécanismes d'authentification tels que des versions électroniques de la pièce d'identité des Forces Canadiennes, de la pièce d'identité des Forces Canadiennes de soins de santé, ou de la pièce d'identité des Forces Canadiennes aux familles des militaires.

Outre les résultats directs de l'évaluation, la méthodologie et le plan d'essai développés dans l'étude, ainsi que le plan du logiciel de test, peut être utilisé pour effectuer la comparaison, plus en profondeur.

Table of contents

List of figures

List of tables

Acknowledgements

This Study was funded through the Centre for Security Science's (CSS) Public Security Technical Program (PSTP). CSS is a joint endeavour between Defence Research and Development Canada (DRDC) and Public Safety Canada.

The authors of the report wish to thank the following individuals:

Ken Canam, Director Architecture and Engineering, CSEC

Pierre Meunier, Portfolio Manager – Surveillance, Intelligence and Interdiction, DRDC

Steven Johnston, Senior Security and Technology Advisor, OPC

Andrew Patrick, Information Technology Research Analyst, OPC

Dmitry Gorodnichy, Senior Research Scientist, CBSA

Mark Labonte, Officer in Charge of Biometric Business Solutions, RCMP

Len Goodman, Defence Scientist, Individual Readiness Section, DRDC-Toronto

Scott Knox, Deputy Director, Physical Security Implementation (ISRP), DFAIT

Ron Cowalchuk, Chief, Security Technology, Research & Development, Transport Canada

Konstantinos Plataniotis, Professor, Electrical and Computer Engineering (ECE) Department, Director, Knowledge Media Institute, U of T / IPSI

This page intentionally left blank.

1 Introduction

This Final Report for the PSTP-02-336BIOM "Assessing Vulnerability of Biometric Technologies for Identity Management Applications" Study describes the purpose, methodology, results, transition and exploitation activities, and conclusions of the activities conducted during the Study. Accompanying it as separate deliverables are:

1. Deliverable A: An analysis of existing biometrics guidance for the IT community

2. Deliverable B: An comparative analysis of biometrics vs. passwords, including a test methodology and plan for conducting a practical evaluation to compare the utility of biometrics vs. passwords, as well as test results and analysis

3. Deliverable C: A guidance document on the implementation of biometric systems aimed at IT practitioners that incorporates a usable framework for addressing biometric vulnerabilities and other deployment factors, and case study examples of real-world deployments of IT System Access applications

The research conducted during this Study aimed to develop a guide for IT security practitioners, who may not be familiar with biometrics as an authentication method, with the intent of addressing the growing use of biometrics in government applications and the implications that it has on information technology (IT) systems security. The Study deliverables include: (1) analysis of existing security management techniques, (2) development of a biometric evaluation framework with relevant case studies, and (3) comparative results of an evaluation of biometric and password security efficacy.

When attempting to compromise an IT system, attackers will generally pursue the easiest point of attack of a particular system. In many cases, this is the point at which the username and password are captured from the user. Mature tools such as Trojan horses and key-loggers that exist in an attacker's arsenal facilitate the collection of passwords.

At the same time, IT deployers may have the "pre-programmed" mindset to utilize usernames and passwords as a method of authentication, due to widespread use, ease of implementation, and comparatively low costs of implementation. Unfortunately, username-password may not be the most secure form of authentication. Thus, when deploying IT systems for IT network access, it is important that organizations examine other valid forms of authentication such as biometrics.

Biometrics has long been used as a method for authenticating people for the purposes of verifying identity and identification. Biometric use in the Federal Government can and is used in physical and logical access applications for the purposes of improving authentication security and ease of use, reducing administrative costs, and providing non-repudiation. Government projects exist that are currently using biometrics, such as the Canadian Air Transport Security Authority's (CATSA) Restricted Area Identification Card (RAIC), as well as those that could potentially use biometrics in the future, such as Canadian Forces Health Information System (CFHIS). These applications utilize biometrics as a method of authentication for applications such as SCADA systems and e-Government services.

The highest-visibility application of biometrics in national government applications is arguably in Civil Identification (ID) applications such as international travel applications including passport issuance and border management, in addition to applications such as national ID programs in certain nations. Further government use of biometrics include employee-facing applications in authentication for IT System Access, particularly network login, and Access Control / Attendance, often in conjunction with smartcard-based employee ID programs. These common government applications are described in more detail in the Study deliverables, along with case studies highlighting current biometric implementations in government settings.

It is important for all organizations, including government agencies, to evaluate and select technology products and services that maintain and improve overall IT security and enterprise architecture. The systematic management of IT security processes is critically important. Failure to consider the many issues involved and to manage the risks can seriously impact the organization. The framework developed during the Study aims to bridge evident gaps in the evaluation of biometric technologies under recognized evaluation criteria, such as the Common Criteria, and will benefit departmental security authorities, IT project managers, IT administrators, security practitioners, and evaluators in assessing the appropriateness of implementing biometric technologies in a government setting, thereby addressing the Study Objectives to:

- Evaluate the potential vulnerability and utility of various biometric technologies for Government use in IT system access control applications (including SCADA systems) and e-Government services; and
- Improve the ability of Canadian Government Agencies to identify and mitigate security vulnerabilities, properly contemplate / mitigate privacy risks, and preserve interoperability.

This Study addresses the following:

1. Reviews general information security mechanisms and the related managerial and administrative issues necessary to ensure confidence in IT security

2. Reviews general security functionality and assurance requirements of IT systems and relevant evaluation criteria

3. Addresses the main functionality and utility factors that should be considered in a biometric technology evaluation

4. Compares the utility factors of biometric technologies to traditional security mechanisms

5. Identifies gaps in current IT security frameworks for the evaluation of biometric technologies

6. Provides a high-level framework for assessing the suitability, limitations, and vulnerabilities of biometric technologies

7. Discusses privacy issues of biometric implementations

8. Details common government applications of biometric technologies and provides government biometric case studies

In order to account for elements that are constantly in flux with the improvement of technology and streamline the focus of this Study, the framework does not:

1. Summarize the current state of biometrics technology or act as a market report

2. Provide specific recommendations on biometric devices and/or modalities

2 Purpose

The first objective of the project was to evaluate the potential vulnerability and utility of biometric technologies for Government use in IT system access control applications and e-Government services. This objective addressed the Biometric community of practice's goal to evaluate, analyze, and support biometric technology implementations that enhance national capabilities.

The second objective was to improve the ability of Canadian Government Agencies to identify and mitigate security vulnerabilities and privacy risks, and preserve interoperability in ID management systems, by producing information for decision-makers with respect to deploying biometric technology as a method for authentication.

The Study addressed the investment category by synthesizing a usable framework for evaluating vulnerabilities in biometric technology options for IT system access control applications and e-Government services. By incorporating existing frameworks and policy documents, this framework provides straightforward guidance for decision-makers deploying authentication and identity management solutions. The framework addresses technical considerations such as vulnerabilities and interoperability, as well as additional deployment factors such as cost, usability, and privacy impact.

The Study included an attempt to directly compare the utility of biometrics and traditional means of single-factor authentication by executing a small-scale evaluation of fingerprint biometrics vs. passwords for desktop application login.

This Study generated and organized knowledge in the form of analyses and guidance, which are encapsulated in the Study deliverables. This knowledge can be used to develop policy and guidance to encourage IT security practitioners to utilize biometric technology as a form or authentication.

3 Methodology

The Project team studied surveyed and analyzed existing reports, guidance, frameworks and analyses related to the deployment of biometric systems for IT network access applications and generated three knowledge-based deliverables:

- An analysis of existing biometrics guidance for the IT community;
- An analysis comparing biometrics to passwords as authentication mechanisms, including an experimental test to compare utility; and
- Guidance on the use of biometrics in network authentication, aimed at IT security practitioners.

3.1 Analysis of Existing Biometrics Guidance and Reports

The project team compiled a list of existing technical reports, guidance, policy, standards and other documents relating to the use of biometrics as an authentication method for IT network access. The team also reviewed documents relating to legal, ethical, cultural and privacy issues related to deployment. Table 1 lists some of the various documents reviewed.

Table 1: Source Documents for Analysis of Existing Guidance and Reports

Title	Organization	Date
Biometric Technology Security Evaluation Under the Common Criteria[1]	CSEC	September 2001
Biometric Application to Government Services Report[2]	CSEC	October 27, 2003
CSE148 DID:CSE03 Government of Canada Biometrics Business Requirements Report[3]	CSEC	March 9, 2004
CSE149 DID:CSE03 Government of Canada Identification and Authentication Framework for Biometric Enabled Applications[4]	CSEC	March 9, 2004
Government of Canada Biometrics Business Case Framework[5]	CSEC	February 9, 2005
BSI-PP-0016 Common Criteria Protection Profile for Biometric Verification Mechanisms[6]	Budesamt für Sicherheit in der Informationstechnik	August 17, 2005
NIST SP 800-63 Electronic Authentication Guideline[7]	NIST Information Technology Laboratory (ITL)	April 2006
INCITS M1/07-0185rev Study Report on Biometrics in E-Authentication[8]	INCITS M1.4 Ad Hoc Group on Biometric in E-Authentication	March 30, 2007
Harmonized Threat and Risk Assessment (TRA) Methodology[9]	CSEC & RCMP	October 23, 2007
ITSG-31 User Authentication Guidance for IT Systems[10]	CSEC	March 2009
ISO/IEC 19792:2009 Security Evaluation of Biometrics[11]	ISO/IEC JTC1 SC 27	August 1, 2009
NIST SP 800-53 Recommended Security Controls[12]	NIST ITL	August 2009
Technical Research Report on Biometrics for	CSEC	March 2010

Authentication for Enterprise Security Architectures[13]		
ITSG-30 Introduction to Guidelines for Information Technology Security in the Government of Canada (Draft 7)[14]	CSEC	December 2010
ITSG-33 Guide to Managing Security Risks (Draft 5)[15]	CSEC	December 2010
ISO/IEC Proposed Draft Technical Report (PDTR) 29156 Guidance for specifying performance (Draft Technical Report)[16]	ISO/IEC JTC1 SC 37	February 2011
Data at Your Fingertips: Biometrics and the Challenges to Privacy[17]	OPC	February 16, 2011

The Study found that while some documents such as the International Committee for Information Technology Standards (INCITS) M1/07-0185rev *Study Report on Biometrics in E-Authentication*[8] had already explored the role for biometric authentication at different assurance levels, as well as the benefits, challenges and threats that accompany the use of biometric authentication and countermeasures, better guidance was needed on the use of biometrics as a replacement for passwords in authentication in a Canadian context. Findings of note included that the INCITS M1 report also provides recommended edits from a biometric practitioner perspective to National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63 *Electronic Authentication Guideline*[7], the U.S. guidance document that discusses the use of biometrics in IT network authentication, and which is one of the key references for ITSG-31 *User Authentication Guidance for IT Systems*[10]; however, these recommended edits have not been implemented by NIST.

The analysis of existing guidance and reports can be found in Deliverable A.

3.2 Analysis comparing Biometrics to Passwords

Using the review of existing biometrics guidance and reports, the Study team conducted a comparison of biometrics and passwords as authentication mechanisms for IT access control. The team produced a report, found in Deliverable B, describing the different types of vulnerabilities in a diagram of an authentication system, and described the vulnerabilities specific to biometrics and passwords.

Additionally, the team developed a test methodology and plan for a small-scale evaluation to compare the utility of biometric authentication to password authentication. The project team built a test platform that simulates the user login experience using a representative fingerprint biometric system and a username-password authentication system, while collecting measurable criteria such as:

- Whether access was granted;
- Number of attempts before gaining access; and
- Time to authenticate.

Data on additional metrics such as ease-of-use and user acceptance were collected using a user survey conducted after the test trials. At the end of the evaluation, the recorded data was aggregated and analyzed.

The test results confirmed experimentally that single-factor biometric technology is a viable and user-accepted means of authentication for IT system access that is at least as fast and accurate as username-password methods. The test results also suggested that the performance of the biometric technology may be better than that of username-password methods in terms of a higher proportion of successful access attempts for daily as well as intermittent use.

The test results and user survey showed that a large number of Test Subjects wrote down their passwords, used “weak” passwords that were easier to remember, and/or used the same password for multiple systems, potentially compromising the strength of the username-password authentication.

These results support the comparative analysis, confirming the utility of a representative biometric technology for IT access control and access to e-Government services, and supporting the primary SOW objective. The results also suggest that decisions to utilize usernames and passwords as an authentication method should be revisited as they may not be as secure in practice as they are assumed to be in theory. However, further study on a larger scale with a larger and more diverse subject population is recommended to strengthen the conclusions.

The analysis comparing biometrics to passwords as authentication mechanisms and the test report can be found in Deliverable B.

3.3 Guidance Aimed at IT Security Practitioners

In consideration of the information security, guidance, and biometric-specific information presented, the Study team drew upon the aforementioned analyses to develop a Biometric Vulnerability Evaluation Framework (BVEF). This multi-level approach is intended to support vulnerability assessments of biometrics as a general solution, in the development of security requirements, in the assurance of specific implementations, and during any follow-on assessments.

The Study team identified gaps in existing guidance and frameworks, and, building upon the CSEC/RCMP *Harmonized Threat and Risk Assessment (TRA) Methodology* [9], added metrics relating to privacy and cost issues.

It is important to note that the guidance developed during this Study is not yet an Information Technology Security Guidance/Guideline (ITSG) document, but simply information that would feed into an official ITSG document.

The guidance on the use of biometrics in network authentication can be found in Deliverable C.

4 Results

4.1 Impact and Relevance

The project outputs, including the biometric vulnerabilities framework, will facilitate the assessment of potential biometric authentication solutions, feeding into new guidance that addresses gaps with respect to the use of biometrics as an authentication mechanism in Canada.

Study results will inform IT security and privacy policy development, and facilitate deployment of biometric technologies as standalone authentication methods and in conjunction with other mechanisms for multi-factor authentication systems.

Results from the comparative evaluation portion of the project will serve as a baseline of data regarding a direct comparison of the utility and usability of biometrics vs. passwords using experimental research trials, opening the door for more comprehensive evaluation scenarios beyond the scope of the Study.

4.2 Lessons Learned and Implementation of Lessons Learned

Study research showed that, while frameworks describing biometric vulnerabilities already exist, they are not optimized for use by IT security practitioners. There is a disconnect between existing frameworks and IT security practitioners in that much of the existing literature is written by members of the biometric community of practice (CoP) for use within that community or are written with an academic audience in mind, instead of an audience of deployers of authentication systems, who may be more familiar with IT security terminology and concepts. At the same time, other frameworks written from a traditional IT security point of view fail to account for the non-deterministic nature of biometric authentication and the unique aspects and issues of biometric technology such as privacy concerns. Thus, a gap exists between available frameworks and their potential audience.

Likewise, guidance for biometrics use in Canada, such as ITSG-31 *User Authentication Guidance for IT Systems*, already exists; however, in the case of ITSG-31, assertions made in the document are not clearly attributed to science-based metrics or are based on U.S. guidelines, which may not be appropriate to Canadian applications.

The framework and guidance developed during this Study attempted to address these gaps.

4.3 New capabilities, partners and networks

The framework represents an improvement in capabilities by providing a usable tool for IT practitioners to use when evaluating whether or not to deploy biometrics as an authentication method for IT network security applications. The Study also aimed to forge stronger connections between IT security and privacy advocates, to discuss issues of mutual concern from different points of view.

5 Transition and Exploitation

5.1 Transition to End Users

In order to transition the results of the Study to end users, the guidance developed during the Study could be incorporated into a CSEC ITSG document. CSEC has responsibility within the Government of Canada to produce guidance on IT security. Thus, creating an ITSG document creates an official reference for potential Canadian deployers of biometric technology. Additionally, guidance surrounding privacy could be incorporated into OPC policy. Both these avenues would help disseminate information to the IT security practitioner community. Active follow-up to educate practitioners could include workshops and presentations at industry conferences.

5.2 Follow-On R&D Recommended

The Study team recommends expanding upon the biometrics vs. passwords test plan and methodology developed during the Study to collect additional empirical and anecdotal data comparing biometrics against passwords and other forms of authentication. The biometrics vs. passwords comparative test methodology developed during the Study is scalable to a larger test involving more complex variables over a longer period of time. Ways to expand the test include:

- Evaluating additional biometric modalities;
- Varying different independent variables;
- Using a larger and more diverse group of test subjects;
- Evaluating multi-factor authentication; and
- Conducting a comparison vs. other types of authentication besides passwords.

Additionally, an even more comprehensive framework for evaluation the use of biometrics in IT network access applications could be developed. This framework would incorporate checklists and decision matrices for evaluating deployments of biometrics in more specific access control scenarios.

6 Conclusion

6.1 Strategic Planning Advice

The Strategic Planning Advice / Advisory Note provides a concise strategic perspective on the project to clearly position its role in the overall public security S&T programs and proposes the strategy for maximizing its success. This particular Study addresses the Surveillance, Intelligence and Interdiction (SI^2) domain need to develop capabilities to "monitor the security environment, understand the threats to national security, and direct an effective and proportionate response to deter, disrupt and stop terrorists and other criminals" by attempting to facilitate increased use of biometrics for authentication in IT network access, thereby deterring and disrupting terrorists and other criminals in the cyber environment. The Study attempted to facilitate increased use of biometrics by developing a reusable analysis capability that could be used by IT security deployers to evaluate the suitability of biometric technologies for their particular authentication needs.

The Strategic Planning Advice was originally presented during the Interim Progress Report meeting. The final Strategic Planning Advice is enclosed as a set of presentation slides.

6.2 Capability Road Map

The Capability Road Map provides a time-sequenced and holistic view of the key "capability inputs or issues" needed to be addressed in order to ensure the success of the project and its overarching goals. The Capability Road Map intentionally includes elements that are out-of-scope for the project, and identifies key activities (capability changes) that are required to adjust the current (as-is) capability with its associated people, processes, and tools to cause it to change incrementally towards a new (to-be) enhanced capability in the future.

6.2.1 PRICIE Framework

Based on direction provided in the *Public Security Technical Program Call No. 2 Proposal Guidebook 2009-2010*, the Capability Road Map builds on capability considerations specified in the PRICIE Framework, whose elements are as follows:

- (P)ersonnel – Human resources required to complete Canada's Department of National Defence (DND) assigned missions and tasks
- (R)esearch & Development (R&D)/Operations Research (O.R.) – R&D are endeavours to increase the knowledge of natural phenomena, the environment and technological resources, O.R. is the scientific field of the collation of information, the transformation of information into knowledge, and the provision of knowledge to decision making
- (I)nfrastructure & Organization – Relation of an organization's size, composition and process to its infrastructure requirements and specifications
- (C)oncepts, Doctrine & Collective Training – Development of ideas and goals followed by the fundamental principles by which the military guide their actions in support of objectives.

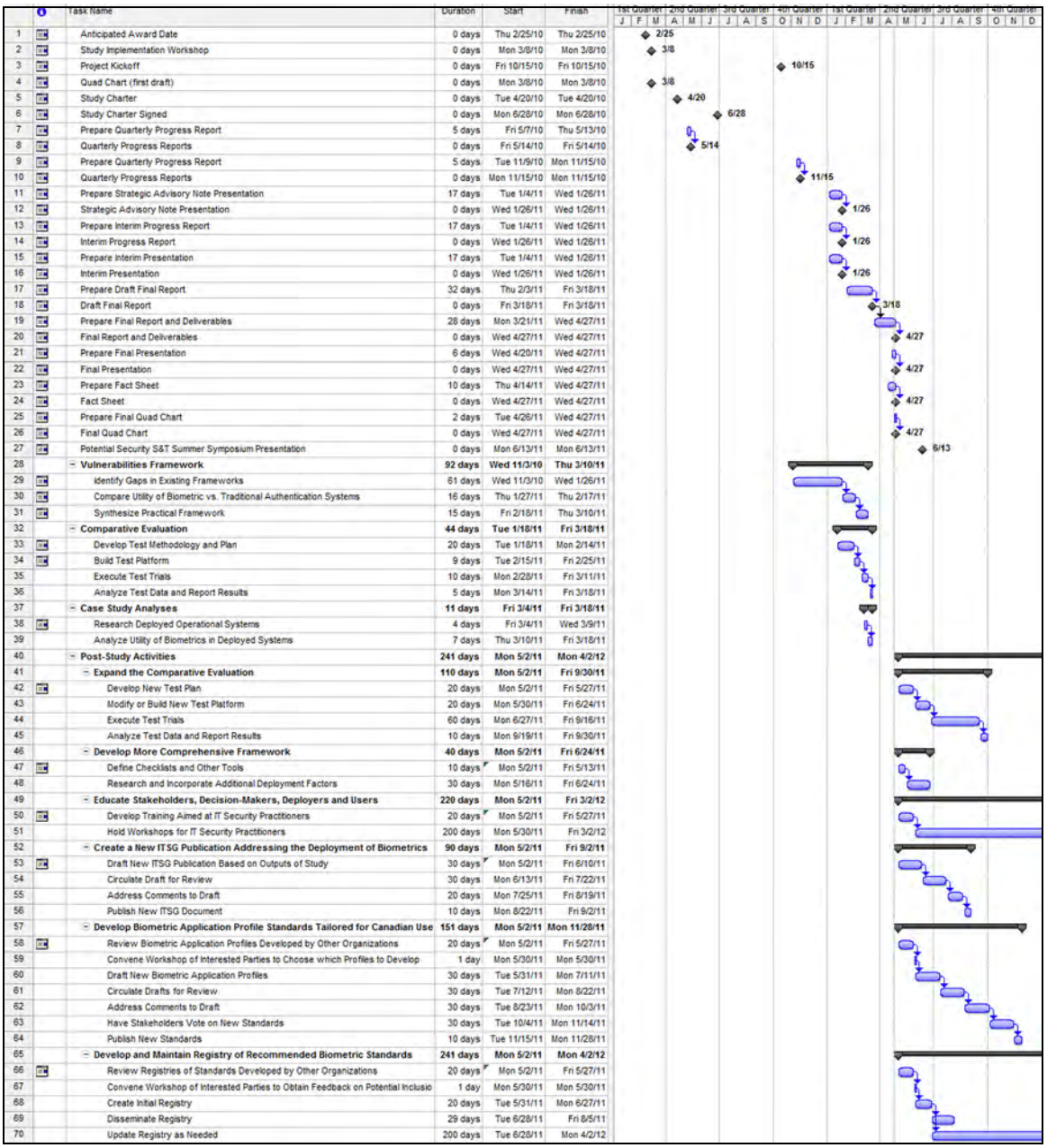
Collective training involves the development of units and formations to generate combat power including lessons learned

- (I)T Infrastructure – Orchestrates the computing, communication, and information systems critical to the rapid development and dissemination of knowledge
- (E)quipment Supplies and Services – Furnishing and maintenance of non-expendable items needed to outfit and individual or organization to accomplish assigned missions or tasks

The PRICIE Framework is intended for analysis of cost models for developmental systems as opposed to research initiatives. As such, certain elements of the Framework are not readily applicable to the current Study. Nonetheless, the Capability Road Map attempts to incorporate key capability inputs across each PRICIE area.

6.2.2 Capability Road Map Chart

Figure 1 depicts a Gantt chart-like schedule that shows the activities executed during the project and potential future elements for that are out-of-scope for the project to reach the Study objectives of: (1) evaluating the potential vulnerability and utility of biometric technologies for Government use in IT system access control applications, and (2) improving the ability of Canadian Government Agencies to identify and mitigate security vulnerabilities and privacy risks, by producing information for decision-makers with respect to deploying biometric technology for authentication. Future activities are listed under “Post-Study Activities”. Note that specific notional tasks and dates listed in the schedule are for illustrative purposes only, and should be superseded by the actual defined tasks in official processes such as standards development processes. Additionally, all potential tasks have been listed as starting immediately following the Study, which may not be realistic or feasible, and finite periods have been used for some ongoing tasks which should continue indefinitely.



	Task Name	Duration	Start	Finish
1	Anticipated Award Date	0 days	Thu 2/25/10	Thu 2/25/10
2	Study Implementation Workshop	0 days	Mon 3/8/10	Mon 3/8/10
3	Project Kickoff	0 days	Fri 10/15/10	Fri 10/15/10
4	Quad Chart (first draft)	0 days	Mon 3/8/10	Mon 3/8/10
5	Study Charter	0 days	Tue 4/20/10	Tue 4/20/10
6	Study Charter Signed	0 days	Mon 6/28/10	Mon 6/28/10
7	Prepare Quarterly Progress Report	5 days	Fri 5/7/10	Thu 5/13/10
8	Quarterly Progress Reports	0 days	Fri 5/14/10	Fri 5/14/10
9	Prepare Quarterly Progress Report	5 days	Tue 11/9/10	Mon 11/15/10
10	Quarterly Progress Reports	0 days	Mon 11/15/10	Mon 11/15/10
11	Prepare Strategic Advisory Note Presentation	17 days	Tue 1/4/11	Wed 1/26/11
12	Strategic Advisory Note Presentation	0 days	Wed 1/26/11	Wed 1/26/11
13	Prepare Interim Progress Report	17 days	Tue 1/4/11	Wed 1/26/11
14	Interim Progress Report	0 days	Wed 1/26/11	Wed 1/26/11
15	Prepare Interim Presentation	17 days	Tue 1/4/11	Wed 1/26/11
16	Interim Presentation	0 days	Wed 1/26/11	Wed 1/26/11
17	Prepare Draft Final Report	32 days	Thu 2/3/11	Fri 3/18/11
18	Draft Final Report	0 days	Fri 3/18/11	Fri 3/18/11
19	Prepare Final Report and Deliverables	28 days	Mon 3/21/11	Wed 4/27/11
20	Final Report and Deliverables	0 days	Wed 4/27/11	Wed 4/27/11
21	Prepare Final Presentation	6 days	Wed 4/20/11	Wed 4/27/11
22	Final Presentation	0 days	Wed 4/27/11	Wed 4/27/11
23	Prepare Fact Sheet	10 days	Thu 4/14/11	Wed 4/27/11
24	Fact Sheet	0 days	Wed 4/27/11	Wed 4/27/11
25	Prepare Final Quad Chart	2 days	Tue 4/26/11	Wed 4/27/11
26	Final Quad Chart	0 days	Wed 4/27/11	Wed 4/27/11
27	Potential Security S&T Summer Symposium Presentation	0 days	Mon 6/13/11	Mon 6/13/11
28	**Vulnerabilities Framework**	**92 days**	**Wed 11/3/10**	**Thu 3/10/11**
29	Identify Gaps in Existing Frameworks	61 days	Wed 11/3/10	Wed 1/26/11
30	Compare Utility of Biometric vs. Traditional Authentication Systems	16 days	Thu 1/27/11	Thu 2/17/11
31	Synthesize Practical Framework	15 days	Fri 2/18/11	Thu 3/10/11
32	**Comparative Evaluation**	**44 days**	**Tue 1/18/11**	**Fri 3/18/11**
33	Develop Test Methodology and Plan	20 days	Tue 1/18/11	Mon 2/14/11
34	Build Test Platform	9 days	Tue 2/15/11	Fri 2/25/11
35	Execute Test Trials	10 days	Mon 2/28/11	Fri 3/11/11
36	Analyze Test Data and Report Results	5 days	Mon 3/14/11	Fri 3/18/11
37	**Case Study Analyses**	**11 days**	**Fri 3/4/11**	**Fri 3/18/11**
38	Research Deployed Operational Systems	4 days	Fri 3/4/11	Wed 3/9/11
39	Analyze Utility of Biometrics in Deployed Systems	7 days	Thu 3/10/11	Fri 3/18/11
40	**Post-Study Activities**	**241 days**	**Mon 5/2/11**	**Mon 4/2/12**
41	**Expand the Comparative Evaluation**	**110 days**	**Mon 5/2/11**	**Fri 9/30/11**
42	Develop New Test Plan	20 days	Mon 5/2/11	Fri 5/27/11
43	Modify or Build New Test Platform	20 days	Mon 5/30/11	Fri 6/24/11
44	Execute Test Trials	60 days	Mon 6/27/11	Fri 9/16/11
45	Analyze Test Data and Report Results	10 days	Mon 9/19/11	Fri 9/30/11
46	**Develop More Comprehensive Framework**	**40 days**	**Mon 5/2/11**	**Fri 6/24/11**
47	Define Checklists and Other Tools	10 days	Mon 5/2/11	Fri 5/13/11
48	Research and Incorporate Additional Deployment Factors	30 days	Mon 5/16/11	Fri 6/24/11
49	**Educate Stakeholders, Decision-Makers, Deployers and Users**	**220 days**	**Mon 5/2/11**	**Fri 3/2/12**
50	Develop Training Aimed at IT Security Practitioners	20 days	Mon 5/2/11	Fri 5/27/11
51	Hold Workshops for IT Security Practitioners	200 days	Mon 5/30/11	Fri 3/2/12
52	**Create a New ITSG Publication Addressing the Deployment of Biometrics**	**90 days**	**Mon 5/2/11**	**Fri 9/2/11**
53	Draft New ITSG Publication Based on Outputs of Study	30 days	Mon 5/2/11	Fri 6/10/11
54	Circulate Draft for Review	30 days	Mon 6/13/11	Fri 7/22/11
55	Address Comments to Draft	20 days	Mon 7/25/11	Fri 8/19/11
56	Publish New ITSG Document	10 days	Mon 8/22/11	Fri 9/2/11
57	**Develop Biometric Application Profile Standards Tailored for Canadian Use**	**151 days**	**Mon 5/2/11**	**Mon 11/28/11**
58	Review Biometric Application Profiles Developed by Other Organizations	20 days	Mon 5/2/11	Fri 5/27/11
59	Convene Workshop of Interested Parties to Choose which Profiles to Develop	1 day	Mon 5/30/11	Mon 5/30/11
60	Draft New Biometric Application Profiles	30 days	Tue 5/31/11	Mon 7/11/11
61	Circulate Drafts for Review	30 days	Tue 7/12/11	Mon 8/22/11
62	Address Comments to Draft	30 days	Tue 8/23/11	Mon 10/3/11
63	Have Stakeholders Vote on New Standards	30 days	Tue 10/4/11	Mon 11/14/11
64	Publish New Standards	10 days	Tue 11/15/11	Mon 11/28/11
65	**Develop and Maintain Registry of Recommended Biometric Standards**	**241 days**	**Mon 5/2/11**	**Mon 4/2/12**
66	Review Registries of Standards Developed by Other Organizations	20 days	Mon 5/2/11	Fri 5/27/11
67	Convene Workshop of Interested Parties to Obtain Feedback on Potential Inclusio	1 day	Mon 5/30/11	Mon 5/30/11
68	Create Initial Registry	20 days	Tue 5/31/11	Mon 6/27/11
69	Disseminate Registry	29 days	Tue 6/28/11	Fri 8/5/11
70	Update Registry as Needed	200 days	Tue 6/28/11	Mon 4/2/12

Figure 1: Capability Road Map

In terms of this Study, the biometric technology for authenticating users in access control applications already exists at a mature, deployable Technology Readiness Level (TRL). What is lacking is clear guidance for deployers, which would provide them with the confidence and justification to deploy it for us in government authentication applications, thereby helping to combat cyber-attacks. Thus, one of the goals was to develop a reusable analysis capability, which can be further extended to include more in-depth risk assessment templates, adding factors such as the cost of remediation.

6.2.3 Current (as-is) Capability

Biometric technology is currently a mature authentication technology, offering several modalities suitable for use in network authentication. Examples of large government programs utilizing biometric technology for authentication exist such as the CATSA RAIC implementation; however, a deficiency in available guidance and education aimed at the IT security community regarding use, especially use in Canada, has prevented widespread deployment. Analysis conducted during the review of existing documents, indicated that the main challenges and gaps toward implementation included:

1. A deficiency in comprehensive, qualified science-based guidance on use of biometrics in authentication systems;

2. A deficiency of straightforward guidance aimed at IT security practitioners and decision-makers; and

3. An absence of active efforts aimed at educating IT security practitioners regarding biometric authentication.

6.2.4 New (to-be) Enhanced Capability

One of the objectives of the Study was to help promote the use of biometric technologies for network authentication amongst IT security practitioners through the development of a reusable analysis capability. Proposed next steps for CSEC would contribute to developing this reusable analysis capability using the Study framework by:

- Expanding the comparative evaluation to collect more empirical and anecdotal data comparing biometrics against passwords and other forms of authentication. The biometrics vs. passwords comparative test methodology developed during the Study is scalable to a larger test involving more complex variables over a longer period of time. Ways to expand the test include:
  - Using additional biometric modalities commonly used for access control (e.g., iris, vein/vascular);
  - Varying different independent variables (e.g., frequency of required password changes);
  - Using a larger and more diverse group of test subjects representing a larger segment of the population (e.g., non-acclimated users, broader age-range);
  - Evaluating multi-factor authentication; and
  - Conducting a comparison vs. other types of authentication (e.g., cryptographic tokens).
- Developing a more comprehensive framework that incorporates:

- Checklists and other tools for evaluating deployments of biometrics in more specific access control scenarios; and
- Additional deployment factors.

- Educating stakeholders, decision-makers, deployers and users to obtain buy-in on the use of the framework by:
  - Developing training materials aimed at IT security practitioners; and
  - Holding workshops for IT security practitioners.
- Utilizing the ITSG development process to create more comprehensive, actionable guidance

Other next steps could include:

- Developing biometric application profile standards tailored for Canadian use; biometric application profiles are currently being developed at the international level, and exist at the U.S. national level.
- Developing and maintaining a registry of Canadian Government recommended biometric standards, similar to the U.S. Government's registry.

6.2.5 Key Activities for Effecting Capability Changes

Challenges exist toward increasing the use of biometric technologies for authentication. These include:

- The need to change the IT security/cryptography mindset that non-deterministic means of authentication are less secure. At the same time, it is important to note that since the Ability to Verify (ATV), which measures the degree to which users can authenticate in a particular system, can never be 100%, deployers must keep in mind that an alternative method must also be deployed.
- Deficiencies in official guidance and education for deployers regarding advantages of biometric authentication such as authenticating the presence of actual users and negative recognition (de-duplication).
- Since biometric systems often require a specialized capture device, an increase in initial start-up costs and ongoing maintenance costs is another potential barrier to deployment.
- Privacy concerns, interoperability, start-up costs and perceived complexity issues continue to be barriers to adoption.

Competitive approaches to authentication equally have drivers and challenges. There have not been many recent technology developments that have improved password authentication systems, although social engineering vulnerabilities are becoming more well-known and therefore addressable through user education. Stronger encryption techniques and the use of salt can be used to protect passwords from certain attacks.

Data collected as part of the user survey after the biometrics vs. passwords comparative evaluation performed during the Study indicated that overall security does not necessarily increase with password strength, enforced by restrictive password rules, since "stronger"

passwords may be more difficult to remember, leading to users writing down passwords, or choosing passwords that may meet restrictive rules, but are nonetheless trivial.

Advances in computing power and decreases in storage cost have made rainbow tables and other password cracking tools and techniques easier to apply, decreasing the overall security of passwords.

6.2.6 People, Processes and Tools

People, processes and tools, which contribute to the general advancement of the state-of-the-art in biometric technology, include challenge problems, government requirements, and competitive evaluations from organizations such as U.S. NIST, which push the envelope, and introduce new modalities. For example, requirements for a compact, mobile ten-print capture scanner device, defined by a consortium of U.S. government agencies led by the U.S. Department of Homeland Security 10 Print Scanner User Group in 2005, spawned a new generation of compact livescan devices from industry. As another example, U.S. NIST is currently benchmarking and attempting to improve the state-of-the-art in face and iris recognition technology through its Multiple Biometric Grand Challenge (MBGC), which aims to "investigate, test and improve performance of face and iris recognition technology on both still and video imagery through a series of challenge problems and evaluation." The people which contribute to these efforts include the government portfolio managers, researchers, technology developers and engineers who define the requirements, execute the evaluations and produce the technologies.

Additionally, general increases in computing speed and memory technologies continually improve overall performance of biometric systems.

People, processes and tools, which could contribute to the goals of the Study of increasing use of biometrics for authentication, include the following:

- Going forward, through its role in producing IT security guidance for the Government of Canada and private industry, CSEC can utilize the existing ITSG development process to create more comprehensive, actionable guidance that IT security practitioners can use. In addition to ITSG documents, guidance can take the form of checklists and procedures as tools that help decision-makers in deciding whether or not biometrics are appropriate for their deployment.
- Members of the biometrics CoP can help promote the results of the Study and the use of biometrics in IT system access control applications within their respective organizations. They can also apply additional tools for spreading the use of biometrics such as: workshops at IT security conferences, disseminating guidance across IT security working groups, and generating internal guidance and memoranda as appropriate.
- To produce guidance that is based on science-based metrics and evaluations, a more in-depth experimental test comparing biometrics to other forms of authentication can be developed and executed. Such a test could be based on the biometrics vs. passwords comparative evaluation performed as part of this Study.

References

References for each of Deliverables A, B and C are found within their respective References sections.

[1] Communications Security Establishment Canada, *Biometric Technology Security Evaluation Under the Common Criteria*. September 2001.

[2] Communications Security Establishment Canada, *Biometric Application to Government Services Report*. 27 October 2003.

[3] Communications Security Establishment Canada, *CSE148 DID: CSE03 Government of Canada Biometrics Business Requirements Report*. 9 March 2004.

[4] Communications Security Establishment Canada, *CSE149 DID: CSE02 Government of Canada Identification and Authentication Framework for Biometric Enabled Applications*. 9 March 2004.

[5] Communications Security Establishment Canada, *Government of Canada Biometrics Business Case Framework*. 9 February 2005.

[6] Budesamt für Sicherheit in der Informationstechnik, *BSI-PP-0016 Common Criteria Protection Profile for Biometric Verification Mechanisms*. 17 August 2005.

[7] NIST ITL, *NIST SP 800-63 Electronic Authentication Guideline*. April 2006.

[8] INCITS M1.4 Ad Hoc Group on Biometric in E-Authentication, *INCITS M1/07-0185rev Study Report on Biometrics in E-Authentication*. 30 March 2007.

[9] Communications Security Establishment Canada and Royal Canadian Mounted Police. *Harmonized Threat and Risk Assessment Methodology*. 23 October 2007.

[10] Communications Security Establishment Canada, *ITSG-31 User Authentication Guidance for IT Systems*. March 2009.

[11] *ISO/IEC 19792:2009 Security Evaluation of Biometrics*. August 2009. <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51521>.

[12] NIST ITL, *NIST SP 800-53 Recommended Security Controls for Federal Information Systems and Organizations*. August 2009. <http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final.pdf>.

[13] Communications Security Establishment Canada, *Technical Research Report on Biometrics for Authentication for Enterprise Security Architectures*. March 2010.

[14] Communications Security Establishment Canada, *ITSG-30 Introduction to Guidelines for Information Technology Security in the Government of Canada (Draft 7)*. December 2010.

[15] Communications Security Establishment Canada, *ITSG-33 Guide to Managing Security Risks (Draft 5)*. December 2010.

[16] *ISO/IEC PDTR 29156 Guidance for specifying performance requirements to meet security & usability needs in applications.* February 2011.

[17] Office of the Privacy Commissioner of Canada, *Data at Your Fingertips: Biometrics and the Challenges to Privacy*. 16 February 2011.

This page intentionally left blank.

Annex A Project Team

Communications Security Establishment Canada (CSEC) served as the lead federal department for the Study, with project partners: IBG-Canada, CBSA, DFAIT, DRDC-Toronto, OPC, RCMP, Transport Canada, U of T / IPSI, GenKey, priv-ID, and Reboot Communications. The following table lists key team members involved in the Study, including the Study Champion and Portfolio Manager.

Role	Name/Title/Organization	Phone Number	E-mail Address
Study Champion (Chair)	Ken Canam, Director Architecture and Engineering, CSEC	613-993-5856	Ken.Canam@cse-cst.gc.ca
Study Project Manager	Drew Smeaton, Manager Research and Prototyping L2C, CSEC	613-991-8081	Drew.Smeaton@cse-cst.gc.ca
Portfolio Manager	Pierre Meunier, Portfolio Manager – Surveillance, Intelligence and Interdiction, DRDC	613-944-4367	Pierre.Meunier@drdc-rddc.gc.ca
Deputy Study Project Manager	Raj Nanavati, Partner, IBG-Canada	647-215-6298	raj@biometricgroup.com
Scientific Expert	Steven Johnston, Senior Security and Technology Advisor, OPC	613-943-2412	sjohnston@privcom.gc.ca
Scientific Expert	Andrew Patrick, Information Technology Research Analyst, OPC	613-996-6791	Andrew.Patrick@priv.gc.ca
Scientific Expert	Dmitry Gorodnichy, Senior Research Scientist, CBSA	613-954-3785	Dmitry.Gorodnichy@cbsa-asfc.gc.ca
Scientific Expert	Mark Labonte, Officer in Charge of Biometric Business Solutions, RCMP	613-993-1749	Mark.A.Labonte@rcmp-grc.gc.ca
Scientific Expert	Len Goodman, Defence Scientist, Individual Readiness Section, DRDC-Toronto	416-635-2125	Len.Goodman@drdc-rddc.gc.ca
Scientific Expert	Scott Knox, Deputy Director, Physical Security Implementation (ISRP), DFAIT	613-996-1888	Scott.Knox@international.gc.ca
Scientific Expert	Ron Cowalchuk, Chief, Security Technology, Research & Development, Transport Canada	613-998-8967	Ron.Cowalchuk@tc.gc.ca
Scientific Expert	Konstantinos Plataniotis, Professor, ECE Department, Director, Knowledge Media Institute, U of T / IPSI	416-946-5605	kostas@comm.utoronto.ca

Annex B Project Performance Summary

B.1 Technical Performance Summary

All milestones for the Study were completed, and all deliverables were delivered. The objectives of the Study were met by initiating scope changes to address them better. These included:

- The focus on links between system performance and security strength of function (SoF) was de-emphasized, as these links were previously explored by other efforts. This was replaced by a more practical comparison of the utility of biometrics vs. passwords.
- The practical evaluation of techniques for enhancing biometric security such as biometric encryption and cancellable templates was de-emphasized. This was replaced with a practical biometrics vs. username/password evaluation, which was more applicable to the objectives of the Study.

B.2 Schedule Performance Summary

Due to contract delays, the project schedule was halved, starting in Q3 instead of Q1. This resulted in a compression of the original schedule. To make up for lost time, instead of conducting the Study phases sequentially, parts of three originally proposed phases were combined, and the biometric vulnerabilities framework was developed concurrently with the evaluation of representative technologies.

B.3 Cost Performance Summary

The Study was completed within the originally proposed budget. During the course of the Study, it was determined that the in-kind contributions of equipment from CSEC, as well as the representative technologies from priv-ID and GenKey, were not appropriate for the realigned focus on the Study. These in-kind amounts were subtracted accordingly.

Annex C Publications, Presentations, Patents

At the time of publication, no additional publications, presentations or patents had been created based on the work of the Study; however, the Study team expects to present results at the Public Security S&T Summer Symposium 2011 in June.

List of symbols/abbreviations/acronyms/initialisms

ASFC	Agence des services frontaliers du Canada
ATV	Ability to Verify
BEM	Biometric Evaluation Methodology
BSI	Budesamt für Sicherheit in der Informationstechnik
BSI-PP-0016	*Common Criteria Protection Profile for Biometric Verification Mechanisms*
BVEF	Biometric Vulnerability Evaluation Framework
CATSA	Canadian Air Transport Security Authority
CBSA	Canada Border Services Agency
CFHIS	Canadian Forces Health Information System
CoP	Community of Practice
CORA	Centre for Operational Research and Analysis
CP	Communauté des praticiens
CSEC	Communications Security Establishment Canada
CSS	Centre for Security Science
CSTC	Centre de la sécurité des télécommunications Canada
DFAIT	Foreign Affairs and International Trade Canada
DND	Department of National Defence
DRDC	Defence Research and Development Canada
ECE	Electrical and Computer Engineering
GRC	Gendarmerie royale du Canada
IBG	International Biometric Group
ID	Identification
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
INCITS M1	*INCITS Technical Committee for Biometrics*
IPSI	Identity, Privacy and Security Institute (University of Toronto)
ISO	International Organization for Standardization
ISO/IEC JTC1/SC 27	*ISO/IEC Joint Technical Committee 1, Subcommittee for IT Security Techniques*
ISRP	Physical Security Implementation Section (DFAIT)

IT	Information Technology
ITL	(NIST) Information Technology Laboratory
ITSG	Information Technology Security Guidance/Guideline
ITSG-31	*ITSG document: User Authentication Guidance for IT Systems*
MAECI	Affaires étrangères et Commerce international Canada
MBGC	Multiple Biometric Grand Challenge
NIST	National Institute of Standards and Technology
NIST SP	NIST Special Publication
O.R.	Operations Research
OPC	Office of the Privacy Commissioner of Canada
PDTR	Proposed Draft Technical Report
PP	Protection Profile (Common Criteria)
PRICIE	Personnel Research and Development and Operations Research; Infrastructure and Organization; Concept, Doctrine and Collective Training; Information Management; and Equipment, Supplies and Services
PSTP	Public Security Technical Program
PTSP	Programme technique de sécurité publique
R&D	Research & Development
RAIC	Restricted Area Identification Card
RCMP	Royal Canadian Mounted Police
RDDC	Recherche et développement pour la défense Canada
SCADA	Supervisory Control And Data Acquisition
SI^2	Surveillance, Intelligence and Interdiction
SISFC	Système d'information de santé des Forces Canadiennes
SOW	Statement of Work
SRI	Surveillance, renseignement et interdiction
TI	Technologies de l'information
TRA	Threat and Risk Assessment
TRL	Technology Readiness Level
U of T	University of Toronto

This page intentionally left blank.

DOCUMENT CONTROL DATA (Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)		
1. ORIGINATOR Drew Smeaton Communications Security Establishment		2. SECURITY CLASSIFICATION UNCLASSIFIED
3.TITLE Assessing Vulnerability of Biometric Technologies for Identity Management Applications: Final Report		
4. AUTHORS Smeaton, D.; Nanavati, R.; Wong, B.; Waung, D.; Coleman, D., Hart, C.; Unwala, A.		
5.DATE OF PUBLICATION October 2011	6a. NO. OF PAGES 37	6b. NO. OF REFS 17
7. DESCRIPTIVE NOTES		
8. SPONSORING ACTIVITY DRDC Centre for Security Science (CRTI/PSTP) Defence R&D Canada 222 Nepean St. 11th Floor Ottawa, ON Canada K1A 0K2		
9a. PROJECT OR GRANT NO. PSTP-02-336BIOM	9b. CONTRACT NO. W2213-116323/001/SS	
10a. ORIGINATOR'S DOCUMENT NUMBER s document.) DRDC CSS CR 2011-19	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.) DRDC CSS CR CR-2011-19	
11. DOCUMENT AVAILABILITY Unlimited		
12. DOCUMENT ANNOUNCEMENT Unlimited		

13.Abstract: To address the Community of Practice (CoP) objective of evaluating the utility of potential biometrics techniques that could be used to enhance the security of Information Technology (IT) systems, including Supervisory Control And Data Acquisition (SCADA) systems and e-Government services, the Study Team for PSTP-02-336BIOM developed a framework for addressing biometric vulnerabilities, researched case study examples of existing deployed biometric systems, and conducted a small-scale evaluation to compare the utility of biometrics vs. passwords.

In developing the framework, the Study Team researched existing biometric evaluation frameworks to identify gaps, and synthesized a practical framework aimed at an audience of IT security practitioners, with the intent of addressing the growing use of biometrics in government applications and the implications that it has on IT systems security.

The Study Team also conducted a preliminary comparative evaluation of the utility of biometrics vs. passwords as a single-factor authentication method using experimental test trials and a user survey. Comparison criteria included: whether or not user access is granted, number of attempts, and usability. The evaluation confirmed experimentally that single-factor biometric technology is a viable and user-accepted means of authentication for IT system access that is at least as fast and reliable as username-password methods.

Résume Pour atteindre l'objectif de la communauté des praticiens (CP) d'évaluer l'utilité des techniques de biométrie qui pourraient être utilisées pour améliorer la sécurité des systèmes informatiques, y compris les systèmes SCADA (télésurveillance et acquisition de données), et les services e-gouvernement, l'équipe d'étude pour PTSP-02-336BIOM a élaboré un cadre pour s'attaquer aux vulnérabilités biométriques, a fait des recherches sur des études de cas des systèmes biométriques existants déployés, et a mené une évaluation à petite échelle pour comparer l'utilité de la biométrie contre les mots de passe.

Dans l'élaboration du cadre, l'équipe d'étude a fait des recherches sur des cadres d'évaluation biométrique existants pour identifier les lacunes, et a synthétisé d'un cadre pratique destiné aux professionnels de la sécurité de technologies de l'information (TI), avec l'intention de s'attaquer à l'utilisation croissante de la biométrie dans les applications gouvernementales et les conséquences qu'elle a sur les systèmes de sécurité de TI.

L'équipe d'étude a également effectué une évaluation comparative préliminaire de l'utilité de la biométrie contre les mots de passe en tant que méthode d'authentification à un seul facteur à l'aide d'essais expérimentaux et une enquête auprès des utilisateurs. Les critères de comparaison ont compris : si ou non l'accès des utilisateurs est accordé, le nombre d'essais, et la facilité d'utilisation. L'évaluation a confirmé expérimentalement que la technologie biométrique seul-doigt est un moyen viable et acceptée par l'utilisateur d'authentification pour l'accès au système informatique qui est au moins aussi rapide et fiable que les méthodes de nom d'utilisateur-mot de passe.

14. KEYWORDS,DESCRIPTORSorIDENTIFIERS
Biometrics; Vulnerabilities; IT Security; Privacy